NSE5_FSM-5.2Q&As

Fortinet NSE 5 - FortiSIEM 5.2

Pass Fortinet NSE5_FSM-5.2 Exam with 100% Guarantee

QUESTION 1

An administrator wants to search for events received from Linux and Windows agents.

Which attribute should the administrator use in search filters, to view events received from agents only.

A. External Event Receive Protocol

B. Event Received Proto Agents

C. External Event Receive Raw Logs

D. External Event Receive Agents

Correct Answer: C

QUESTION 2

What is a prerequisite for a FortiSIEM supervisor with a worker deployment, using the proprietary flat file database?

A. The CMDB database must be on NFS

B. The event database must be on NFS

C. The event database must be on a local disk

D. The \archive mount must be on a local disk

Correct Answer: B

QUESTION 3

If the reported packet loss is between 50% and 98%. which status is assigned to the device in the Availability column of summary dashboard?

A. Down status is assigned because of packet loss.

B. Up status is assigned because of received packets

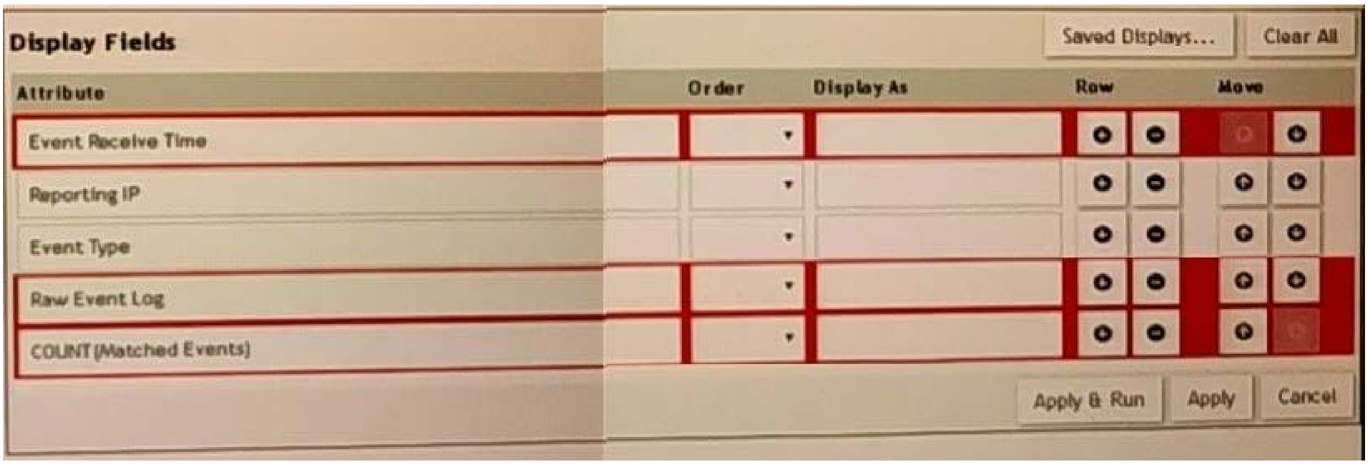
C. Critical status is assigned because of reduction in number of packets received

D. Degraded status is assigned because of packet loss

Correct Answer: D

QUESTION 4

Refer to the exhibit.



Display Fields

Attribute	Order	Display As	Row	Move
Event Receive Time				
Reporting IP				
Event Type				
Raw Event Log				
COUNT (Matched Events)				

A FortiSIEM administrator wants to group some attributes for a report, but is not able to do so successfully. As shown in the exhibit, why are some of the fields highlighted in red?

A. The Event Receive Time attribute is not available for logs.

B. The attribute COUNT(Matched event) is an invalid expression.

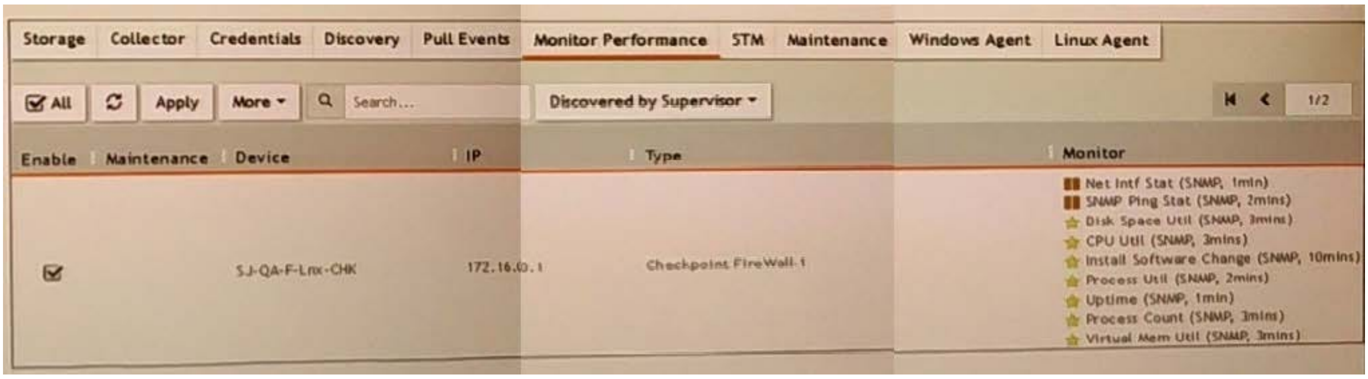
C. Unique attributes cannot be grouped.

D. No RAW Event Log attribute is available for devices.

Correct Answer: C

QUESTION 5

Refer to the exhibit.



Enable	Maintenance	Device	IP	Type	Monitor
☑		SJ-QA-F-Lnx-CHK	172.16.0.1	Checkpoint FireWall-1	Net Intf Stat (SNMP, 1min) SNMP Ping Stat (SNMP, 2mins) ☆ Disk Space Util (SNMP, 3mins) ☆ CPU Util (SNMP, 3mins) ☆ Install Software Change (SNMP, 10mins) ☆ Process Util (SNMP, 2mins) ☆ Uptime (SNMP, 1min) ☆ Process Count (SNMP, 3mins) ☆ Virtual Mem Util (SNMP, 3mins)

What do the yellow stars listed in the Monitor column indicate?

A. A yellow star indicates that a metric was applied during discovery, and data has been collected successfully

B. A yellow star indicates that a metric was applied during discovery, but data collection has not started

C. A yellow star indicates that a metric was applied during discovery, but FortiSIEM is unable to collect data.

D. A yellow star indicates that a metric was not applied during discovery and, therefore, FortiSEIM was unable to collect data.

Correct Answer: D